ABSTRACT OF THE DISCLOSURE

The invention is to provide a group lock which is used in group units for encryption, decryption, and signature. A public key, private key, and common key are provided and the private key is encrypted by use of the common key. The common key is encrypted by use of each public key of the group/member. A group lock which includes the public key, a cryptogram of the private key, and a plurality of cryptograms of the common key is generated. The group/member acquires the group lock and decrypts the cryptograms of the common key by use of the private key of the subject itself to acquire the common key, and decrypts the cryptogram of the private key of the group lock to acquire the private key. The group/member acquires the cryptogram which is encrypted by use of the public key of the group lock sent to the group and decrypts the cryptogram by use of the decrypted private key.